فصلنامه علمی - پژوهشی فرماندهی و کنترل، سال چهارم، شماره دو، تابستان ۱۳۹۹

ارائه الگوریتم احراز هویت فرستنده‌های رادیویی مبتنی بر رفتار غیرخطی تقویت کننده توان

علی ناصری[1]، سید رضا طباطبایی منش[2]

تاریخ پذیرش: ۱۳۹۹/۰۴/۲۱ تاریخ دریافت: ۱۳۹۹/۰۸/۱۳

چکیده

در یک فرایند تولید قطعات الکترونیکی هیچ وقت قطعات تولیدی کاملا مشابه نیستند. این موضوع باعث می‌شود سیگنال خروجی از فرستنده‌های رادیویی(حتی فرستنده های رادیویی مشابه) با هم متفاوت باشند. این تفاوت‌ها ناچیز است بنابراین استانداردهای مخابراتی را نقض نمی‌کنند ولی می‌توان از این تفاوت‌های ذاتی و یکتا به عنوان ویژگی‌های لایه فیزیکی برای احراز هویت فرستنده‌های رادیویی بهره برد. به طور معمول احراز هویت‌های نرم‌افزاری قابل جعل است. جعل احراز هویت بر اساس ویژگی‌های ذاتی رادیوها بسیار مشکل و یا غیر ممکن است. زیرا این کار به دانش، هزینه و زمان زیاد نیاز دارد. تقویت کننده توان آخرین بخش فرستنده می‌باشد پس بیشترین اثر را روی سیگنال خروجی فرستنده می‌گذارد. در تحقیق‌های قبلی، گیرنده با فرض دانستن مقدار SNR سیگنال دریافتی، از ضرایب مدل غیرخطی تقویت کننده توان برای طبقه‌بندی فرستنده ها استفاده شده است. در این مقاله یک ویژگی جدید ارائه شده تا عملیات احراز هویت، مستقل از مقدار SNR سیگنال دریافتی انجام شود. نتایج شبیه‌سازی نشان می‌دهد که با استفاده از ویژگی جدید ارائه شده، فرآیند احراز هویت فرستنده رادیویی برای مقادیر SNR کم (حداقل 15 dB) تا زیاد، بدون نیاز به اندازه‌گیری SNR، به خوبی با احتمال موفقیت بیش از ۸۰٪ انجام می‌شود.

کلمات کلیدی: احراز هویت، رادیو، تقویت کننده توان، مدل، غیرخطی، فرستنده، لایه فیزیکی، ویژگی ذاتی، الگوریتم، SNR

[1] دانشیار دانشگاه جامع امام حسین(ع)، نویسنده مسئول، anaseri@ihu.ac.ir

[2] پژوهشگر جامعه دانش بنیان رشد

۱– مقدمه

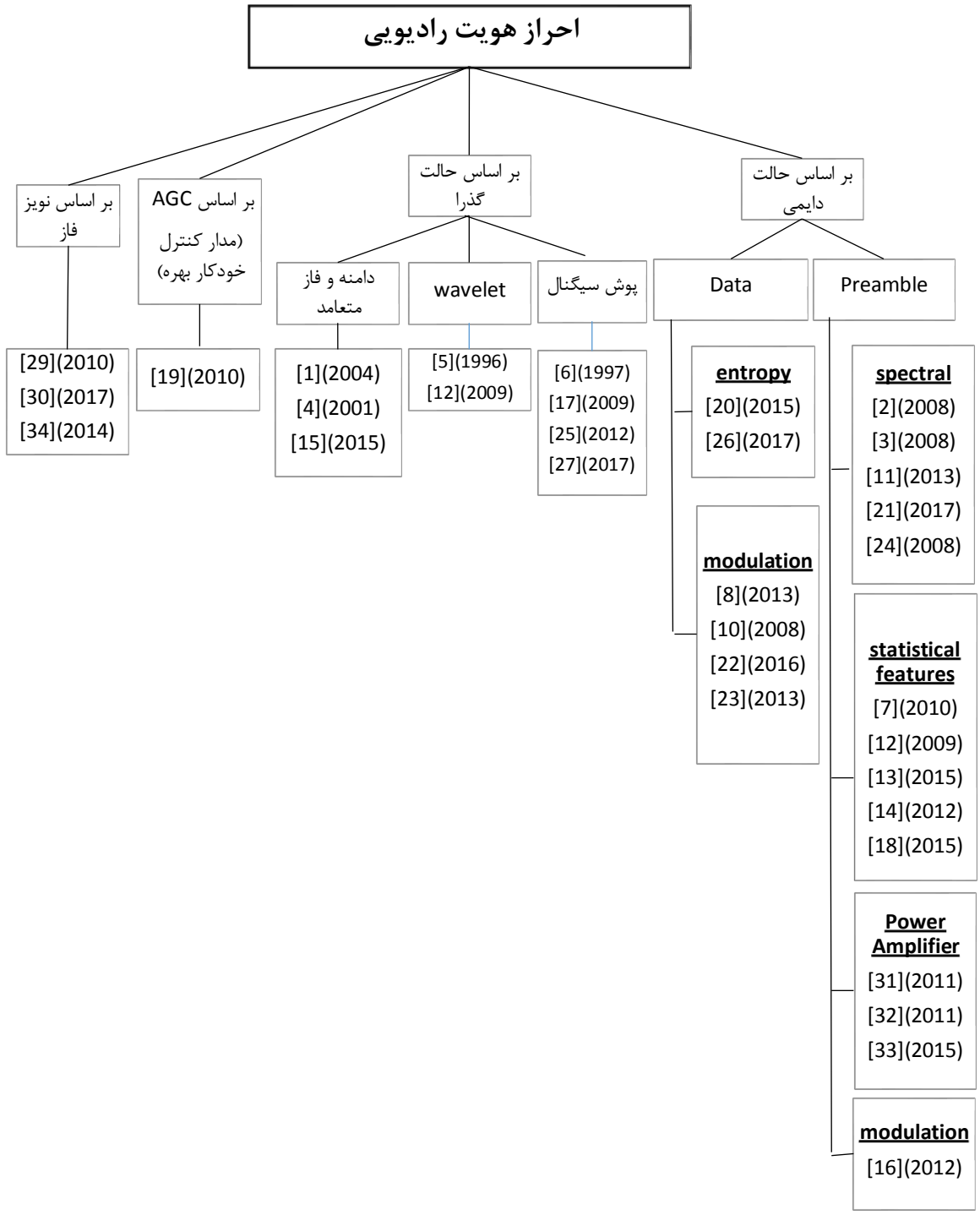
ارتباطات رادیویی یکی از مهمترین بخش‌ها در ارتباطات به شمار می‌آیند. لینک‌های ارتباط رادیویی به صورت استاتیکی و تاکتیکی در سطوح مختلف بخش دفاعی و غیر دفاعی کاربرد دارند. امروزه شبکه سازی رادیوها در قالب شبکه‌های تاکتیکی در بخش دفاعی و شبکه‌های سلولار در بخش تجاری نقطه عطفی برای ارتباطات رادیویی شده است به صورتی که نقش محوری در ارتباطات آحاد جامعه بشری بازی می‌کند. ظهور و بروز خدمات الکترونیکی از یک طرف و راهبرد دریافت این خدمات در هر شرایطی توجه محققین را به دریافت این خدمات مبتنی بر موبایل معطوف ساخت. بخش عمده‌ای از خدمات الکترونیکی از جمله خدمات مالی و حقوقی و دفاعی نیازمند امنیت همه جانبه می‌باشند. امنیت هم در برگیرنده تبادلات رمز شده و هم احراز هویت دو طرف است. خیلی از افراد نفوذگر چه در گروه‌های ساختار یافته و چه در گروه‌های غیر ساختاریافته برای نفوذ بایستی از ضعف‌های سامانه و پروتکل‌های احراز هویت بهره ببرند. بنابراین در ابتدا مراحل نفوذ بر ضعف‌ها و آسیب پذیری‌های سامانه احراز هویت متمرکز می‌شوند. امروزه احراز هویت مبتنی بر الگوریتم‌های احراز هویت است. محققین جهانی به سمت احراز هویت بدون به کارگیری پروتکل‌های سنتی احراز هویت می‌رود، چون در این الگوریتم‌ها که بر پایه ارسال کد و رمز می‌باشند، احتمال فریب در آنها بسیار زیاد است. گزارش‌های زیادی در خصوص آسیب پذیری‌های این سامانه‌ها در دنیا منتشر شده است و هر روز شاهد آسیب پذیری‌های بیشتر این سامانه‌ها هستیم. اخیراً تأمین امنیت در لایه فیزیکی ارتباطات مدنظر محققین قرار گرفته است. یکی از پارامترهای تأمین امنیت در لایه فیزیکی، احراز هویت رادیویی است که در قالب امضاء رادیویی مطرح می‌شود. ولی احراز هویت بر اساس مشخصات رادیویی از مشخصات ذاتی فرستنده استفاده می‌کند و احتمال فریب بسیار کاهش پیدا می‌کند. در مخابرات بی‌سیم، امواج فیزیکی که توسط هر دستگاه بی‌سیم فرستاده می‌شوند، به طور ذاتی تحت تأثیر ویژگی‌های یکتای لایه فیزیکی مخابرات قرار می‌گیرند، که از این ویژگی‌ها می‌توان برای احراز هویت و دسته بندی کاربران واقعی استفاده کرد. اینگونه راه‌حل‌ها برای احراز هویت دستگاه‌ها، به صورت تکنیک‌های احراز هویت لایه فیزیکی بی‌سیم تعریف می‌شود. بر خلاف احراز هویت متداول در سطح نرم افزار دستگاه‌ها (مثلاً IP و آدرس MAC) که به راحتی قابل تغییر هستند، مشخصات لایه فیزیکی به این راحتی‌ها قابل تغییر نیستند. در فرستنده رادیویی، ویژگی‌های منحصر به فرد موج رادیویی مانند: نویز فاز نوسانگر، خطای نمونه برداری مبدل دیجیتال به آنالوگ، الگوی انتشاری آنتن فرستنده و مشخصه غیرخطی میکسر و تقویت کننده توان، در اثر اختلاف‌های جزیی ناشی از خطاهای اجتناب ناپذیر روند ساخت قطعات سخت افزاری به وجود می‌آیند. در گیرنده، سیگنال‌های فرستنده توسط آنتن گیرنده دریافت می‌شوند و توسط مدارات آنالوگ و دیجیتال تجزیه و تحلیل می‌شوند. بسته به سیگنال، ویژگی‌های مختلفی از بخش‌های مختلف سیگنال مانند حالت گذرا، دیتا و ساعت، در حوزه‌های مختلف مانند زمان، فرکانس و ویولت استخراج می‌شوند.

۲–روش‌های احراز هویت رادیویی

بررسی های کارشناسی حاکی از آن است که درخت‌واره فعالیت‌های امضاء رادیویی به شرح شکل۱ می‌باشد. روش‌هایی را که تا کنون محققین برای احراز هویت رادیویی استفاده کرده‌اند را می‌توان به چهار دسته اصلی

تفکیک نمود. این چهار روش اصلی عبارتند از: احراز هویت رادیویی فرستنده بر اساس حالت گذرا [۱،۴،۵،۶،۱۲،۱۵،۱۷،۲۵،۲۷]، احراز هویت رادیویی فرستنده بر اساس حالت دایمی [۲،۳،۷،۸،۱۰،۱۱،۱۲،۱۳،۱۴،۱۸،۲۰،۲۱،۲۲،۲۳،۲۴،۲۶،۳۱،۳۳] ، احراز هویت رادیویی فرستنده بر اساس نویز فاز [۲۹،۳۰،۳۴] و احراز هویت رادیویی فرستنده بر اساس مدار کنترل خودکار بهره [19].

روش‌های بر پایه حالت گذرا قدیمی‌ترین روش‌های احراز هویت رادیویی فرستنده هستند[4]. اساس عملکرد این روش استخراج ویژگی‌های شکل موج حالت گذرای سیگنال، مانند شیب و زمان حالت گذرا است. این روش برای مدولاسیون آنالوگ هم قابل استفاده است و در صورتی که آغاز و پایان حالت گذرا به خوبی تشخیص داده شود، عملکرد طبقه‌بندی خوبی را ارائه می‌دهد[25]. عیب این روش این است که برای تشخیص محل حالت گذرا به SNR نسبتاً بالا و تغییر ناگهانی دامنه در محل شروع حالت گذرا نیاز است، که در عمل ممکن است تغییر ناگهانی دامنه وجود نداشته باشد و SNR کم باشد[2]. همچنین مقدار کم توان ارسالی سیگنال در حالت گذرا و مدت زمان کم این سیگنال، عملکرد گیرندگی این سیگنال و تمایز بین فرستنده‌های هم مدل را دشوار می‌کنند. توصیف شکل موج حالت گذرا به شکل ساده چالش برانگیز است و شناسایی حالت گذرا به نرخ نمونه برداری بالا و گیرنده‌های گران قیمت و پیچیده (اسیلوسکوپ و تحلیلگر طیف) نیاز دارد[11,24]. با وجود اینکه خروجی یک نوسانگر به طور ایده‌آل یک سیگنال سینوسی است، در عمل نوسانگرها یک سیگنال شبه سینوسی تولید می‌کنند که دارای فاز و انحراف فرکانسی متغیر با زمان است. فاز متغیر با زمان سیگنال شبه سینوسی (که نویز فاز نامیده می‌شود) و انحراف فرکانسی از ویژگی‌های ذاتی و یکتای نوسانگر هستند، بنابراین می‌توان با ارسال سیگنال نوسانگر به گیرنده و مدلسازی این ویژگی‌ها، عملیات احراز هویت فرستنده را بر اساس پارامترهای مدل نویز فاز انجام داد[34]. روش شناسایی بر اساس مدل نویز فاز سیگنال نوسانگر محلی، با مدت زمان کوتاه سیگنال ضبط شده و SNR نسبتاً کمتر، سازگاری دارد و به سطح توان سیگنال حساسیت کمی دارد. عیب این روش این است که نیاز به ارسال سیگنال جداگانه نوسانگر محلی توسط فرستنده دارد که باعث افزایش پهنای باند مصرفی شده و هزینه را افزایش می‌دهد و در استانداردهای رادیویی کنونی این قابلیت وجود نداشته و پیش بینی نشده است[30].



شکل ۱: درخت‌واره روش‌های احراز هویت رادیویی

روش‌های احراز هویت رادیویی فرستنده بر اساس حالت دایمی انواع گوناگونی دارد. این روش‌ها بر اساس استخراج ویژگی‌های حالت دایمی سیگنال مانند دامنه، فاز و فرکانس عمل می‌کنند[12]. بهره-گیری از ویژگی‌های مدولاسیون سیگنال‌های ارسالی در روش‌های مبتنی بر حالت دایمی اهمیت ویژه‌ای دارد. سیگنال‌های حوزه مدولاسیون ساختار مناسبی دارند و توصیف موجز این سیگنال‌ها ساده است، ولی روش شناسایی بر اساس حوزه مدولاسیون به اطلاع قبلی از مشخصات مدولاسیون سیگنال ارسالی نیاز دارد[10] و علاوه بر این، ویژگی‌های فرستنده که از سیگنال ارسالی استخراج شده‌اند، به نوع مدولاسیون

بستگی دارند و در باند پایه قابل تغییر هستند[40]. روش شناسایی بر اساس سیگنال آغازین[1] نیازی به دمدولاسیون سیگنال ندارد ولی عیب این روش این است که در بسیاری از کاربردها امکان دارد سیگنال آغازین وجود نداشته باشد یا استخراج آن دشوار باشد[20]. عملکرد روش شناسایی بر اساس تبدیل موجک[2] به انتخاب توابع پایه تبدیل موجک بستگی دارد[20] و این روش به سیگنال آغازین نیاز است[12].

روش شناسایی بر اساس مدار کنترل خودکار بهره نیاز به آگاهی زیادی از ساختار درونی مدار کنترل خودکار بهره در گیرنده دارد. در این روش چگونگی تغییر بهره نسبت به زمان، در پاسخ به سیگنال آغازین ارسالی از فرستنده، مبنای شناسایی فرستنده می‌باشد. همچنین پاسخ این مدار کنترل خودکار بهره به سیگنال یک فرستنده مشخص، متغیر با زمان است، که این مشکلات نشان‌دهنده ناکارآمدی این روش است[19].

تقویت کننده‌های توان به دلیل اینکه آخرین المان فرستنده هستند، بیشترین اثر غیرخطی فرستنده را تولید می‌کنند و اصلاح این اثرها به صورت نرم افزاری و در باند پایه، سخت‌تر از جبران اثرهای دیگر توسط کاربر است، بنابراین در بین روش‌های مبتنی بر حالت دایمی، بهره‌گیری از ویژگی‌های غیرخطی تقویت کننده توان برای احراز هویت فرستنده مورد توجه قرار گرفته است. در روش شناسایی فرستنده بر اساس مدل غیرخطی تقویت کننده توان در فرستنده، به ارسال توان زیاد توسط فرستنده برای تشخیص محل شروع حالت گذرا نیازی نیست (بر خلاف روش‌هایی که از حالت گذرای سیگنال فرستنده برای شناسایی بهره می‌برند) و با نسبت‌های توان سیگنال به نویز کم 15dB تا 20dB هم کار می‌کنند. همچنین این روش با مدولاسیون‌های مختلف سیگنال سازگاری دارد. در این روش سیگنال اطلاعات ارسالی فرستنده، توسط گیرنده تخمین زده شده و بازیابی می‌شود و نیازی به ارسال و شناسایی سیگنال استاندارد یکسان (سیگنال آغازین) در ابتدای پیام‌های همه فرستنده‌ها برای شناسایی، ندارد.

در [31] از ضرایب مدل غیرخطی تقویت کننده توان که آخرین المان فعال فرستنده است، به عنوان ویژگی‌های ذاتی فرستنده رادیویی برای دسته‌بندی[3] فرستنده‌ها استفاده می‌شود. در این مقاله با استفاده از این ویژگی‌های ذاتی، احراز هویت[4] و تشخیص معتبر یا جعلی بودن سیگنال فرستنده رادیویی انجام شده است. در [37] نشان داده شده است که عملکرد فرآیند شناسایی به فاصله بین فرستنده و گیرنده و در نتیجه SNR سیگنال دریافتی، بستگی زیادی دارد.در این مقاله، در ابتدا برای کاهش اثر کانال AWGN از میانگین ضرایب مدل غیر خطی استفاده شده است. سپس برای از بین بردن وابستگی عملکرد این روش به مقدار SNR، با استفاده از مقادیر میانگین و انحراف معیار ضرایب مدل غیرخطی، یک پارامتر جدید تعریف شده است که در مقایسه با [35] که در آن از روش یادگیری عمیق استفاده شده است، پیچیدگی کمتری دارد و قابلیت تغییر مدل غیرخطی، بدون تغییر الگوریتم پیشنهادی، به سادگی قابل انجام است.

۳–الگوریتم پالک و همکاران

الگوریتم ارائه شده توسط پالک و همکاران که در مرجع [31] آمده، طبقه‌بندی فرستنده‌های رادیویی را مبتنی بر ویژگی‌های غیرخطی تقویت کننده توان که جزو روش‌های حالت دایمی احراز هویت می‌باشد، انجام می‌دهد. بر اساس [۳۱] رابطه ورودی فرستنده رادیویی و ورودی گیرنده رادیویی به صورت زیر تعریف می‌شود:

$$Y_i = P_i H_i + N_i \qquad ;i = 1,2,...,m,...,L \quad (1)$$

[1] Preamble
[2] Wavelet
[3] Classification
[4] Identification

که i شماره فرستنده و P_i ماتریسی است که درایه‌های آن توابع غیر خطی از بردار ورودی فرستنده X_i هستند. این توابع بر اساس مدل غیرخطی که برای تقویت کننده‌های توان در نظر گرفته می‌شود، تعیین می‌گردد و برای تمام فرستنده‌های مورد آزمایش یکسان است. بردار H_i که ضرایب مدل غیرخطی می‌باشد، برای هر تقویت کننده توان یکتا است و بر اساس آن ویژگی هر فرستنده تعیین می‌گردد. N_i بردار نویز گوسی سفید جمع شونده[1] است. در واقع حاصل ضرب $P_i H_i$ خروجی فرستنده است که پس از عبور از کانال نویزی AWGN، Y_i را می‌سازد که Y_i سیگنالی است که گیرنده دریافت می‌کند و نمونه‌های بردار ورودی فرستنده X_i را از روی آن بازیابی می‌کند. مشاهده می‌شود که تنها برداری که باید برای احراز هویت کاربر i -ام تخمین زده شود، بردار H_i است.

هدف از فرآیند شناسایی اطمینان از هویت سیگنال فرستنده، می‌باشد. در فرآیند شناسایی، معتبر بودن و یا اصطلاحاً خودی بودن سیگنال ورودی به گیرنده، تشخیص داده می‌شود. در این فرآیند E_1 فرضیه این است که اثر انگشت رادیویی سیگنال آزمایشی ورودی مربوط به یک فرستنده معتبر است. در صورتی که E_0 فرضیه این است که اثر انگشت رادیویی سیگنال آزمایشی مربوط به یک فرستنده نامعتبر است.

حال بر اساس فاصله بردار ویژگی اثر انگشت رادیویی سیگنال آزمایشی ورودی (S) از بردار ویژگی اثر انگشت رادیویی سیگنال فرستنده مرجع (S_R)، یک حد آستانه تصمیم گیری λ تعیین می‌شود. بردار ویژگی اثر انگشت رادیویی سیگنال فرستنده مرجع (S_R) در آزمایشگاه با SNR اندازه‌گیری شده و در حافظه گیرنده ذخیره می‌شود.

$$D(S)=\text{Distance}(S,S_R) \qquad (2)$$

$$D(S) \underset{E_1}{\overset{E_0}{\gtrless}} \lambda \qquad (3)$$

با توجه به رابطه بالا، به کمک مقایسه فاصله بردار ویژگی سیگنال آزمایشی و سیگنال مرجع با مقدار حد آستانه، می‌توان فرآیند شناسایی را انجام داد[37]. برای ارزیابی دقت عملکرد فرآیند شناسایی، چند سنجه احتمالاتی شرطی را می‌توان به کار برد که عبارتند از:

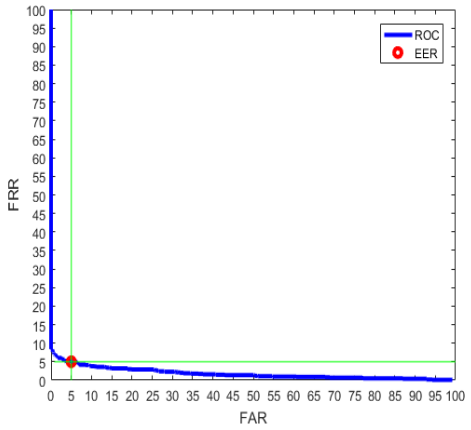
$$\text{False Accept Rate } (\text{FAR})=\text{P}(\text{E}_1|\text{E}_0) \qquad (4)$$

$$\text{False Reject Rate } (\text{FRR})=\text{P}(\text{E}_0|\text{E}_1) \qquad (5)$$

$$\text{Genuine Accept Rate } (\text{GAR})=\text{P}(\text{E}_1|\text{E}_1) \qquad (6)$$

$$\text{Genuine Reject Rate } (\text{GAR})=\text{P}(\text{E}_0|\text{E}_0) \qquad (7)$$

برای ایجاد یک معیار، در برخی از تحقیق‌ها، سنجه‌های بالا در یک نمودار مشخصه گیرنده[2] (ROC) رسم می‌شوند. همانطور که در شکل ۲ نمایش داده شده است، FRR بر اساس تابعی از سطوح مختلف FAR رسم می‌شود. نقطه‌ای در نمودار ROC که FAR و FRR برابر هستند، نرخ خطای برابر[3] (EER) نامیده می‌شود [37]. در [37] مشاهده می‌شود که در فرآیند احراز هویت، λ تابعی از مکان فرستنده نسبت به گیرنده و در نتیجه تابعی از مقدار SNR است. در این مقاله برای رفع وابستگی مقدار λ به مقدار SNR، یک ویژگی جدید پیشنهاد می‌شود.



[1] Additive White Gaussian Noise (AWGN)

[1] Receiver Operating Characteristic chart(ROC)
[3] Equal Error Rate(EER)

شکل ۲: یک نمونه از نمودار ROC (SNR=25 dB و EER=5%)

۴-الگوریتم پیشنهادی

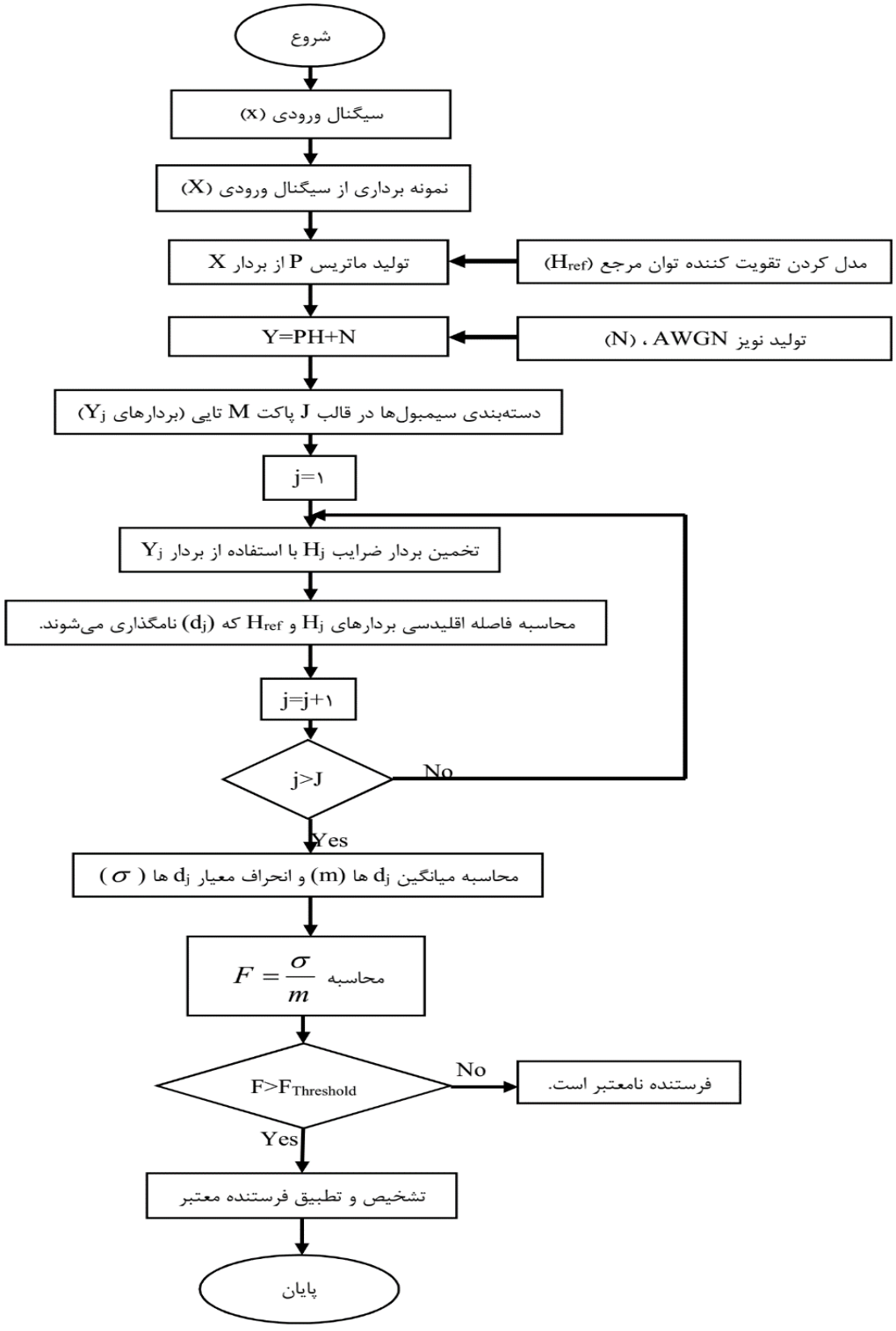
در عمل تقویت کننده‌های توان در ناحیه غیرخطی کار می‌کنند که باعث می‌شود که پاسخ تقویت کننده توان نیز غیر خطی باشد. به همین دلیل نیاز است که در بحث احراز هویت رادیویی به کمک ویژگی‌های غیرخطی فرستنده، از یک مدل غیرخطی به اندازه کافی دقیق استفاده کنیم. در مقاله‌های تحقیقی، مدل‌های غیرخطی تقویت کننده توان به طور معمول به دو دسته مدل‌های رفتاری (مدل‌های جعبه سیاه) و مدل‌های توصیف فیزیکی، تقسیم می‌شوند. در مدل‌های توصیف فیزیکی لازم است که ساختار داخلی تقویت کننده و مقادیر المان‌های مدار داخلی و تاثیرات متقابل آنها را بدانیم. این مدل‌ها برای طراحی تقویت‌کننده در سطح مدار به کار می‌روند و شبیه‌سازی آنها بسیار زمان‌بر است. در مدل‌های رفتاری، به تقویت کننده توان (یا فرستنده) به عنوان یک جعبه سیاه نگاه می‌شود، یعنی ساختار داخلی تقویت کننده توان را نمی‌دانیم یا دانستن آن لازم نیست. در این روش که به طور گسترده در مقاله‌های تحقیقاتی استفاده می‌شود، مدل‌سازی تنها بر اساس مشاهده سیگنال ورودی و خروجی تقویت کننده توان است. مدل‌های رفتاری تقویت کننده توان غیرخطی را می‌توان به سه نوع تقسیم‌بندی کرد:

۱) بدون حافظه ۲) شبه بی‌حافظه ۳) حافظه‌دار

مدل چند جمله‌ای غیرخطی بی‌حافظه و مدل Rapp نمونه‌هایی از مدل‌های بی‌حافظه هستند. مدل Saleh، مدل Ghorbani و مدل تانژانت هایپربولیک مثال‌هایی از مدل‌های رفتاری شبه بی‌حافظه هستند. مدل سری ولترا و حالت‌های خاص و ساده‌تر سری ولترا مانند مدل Wiener، مدل Hammerstein، مدل Wiener-Hammerstein و مدل چند جمله‌ای غیرخطی حافظه‌دار بسط یافته، مدل‌های رفتاری حافظه‌دار هستند[38]. مدل‌های Hammerstein و Wiener تعداد پارامترهای کمتری نسبت به مدل ولترا دارند. ولی مدل چند جمله‌ای حافظه‌دار، مصالحه خوبی را بین عمومیت مدل، آسانی تخمین پارامترهای مدل و سهولت پیاده‌سازی برقرار می‌کند. بر اساس [۳۶] مدل چند جمله‌ای غیرخطی حافظه‌دار بسط یافته بهترین مصالحه را بین پیچیدگی و دقت دارد.

الگوریتم پیشنهادی برای شناسایی فرستنده‌های رادیویی که مبتنی بر الگوریتم پالک و همکاران [31] می‌باشد، در شکل ۳ در ادامه توضیح داده شده است. در ابتدا از سیگنال آنالوگ ورودی (x) نمونه برداری می‌شود تا سیگنال ورودی دیجیتال (X) ساخته شود. سیگنال X، سیگنال گوسی با میانگین صفر و انحراف معیار σ_X است. بر اساس [31] با انتخاب انحراف معیار استاندارد برابر $\sigma_X = 0.055$، با توجه به اینکه بهره توان تقویت کننده 30dB است، احتمال اینکه دامنه سیگنال ورودی از محدوده خطی ورودی تقویت کننده مورد نظر که 7dBm- است، بیشتر شود، ۰.۱٪ است. بنابراین برای تقویت‌کننده‌ای که در این مقاله در نظر گرفته شده است، $\sigma_X = 0.055$ در نظر گرفته می‌شود. سپس بر اساس نوع مدلی که برای مدلسازی تقویت کننده توان در نظر گرفته شده است، ماتریس P از بردار X ساخته می‌شود. ماتریس P دارای D ردیف و C ستون است. D تعداد سیمبول‌های نمونه برداری شده سیگنال X است و C تعداد ضرایب مدل غیرخطی تقویت کننده توان یا همان طول بردار H_{ref} است. در این مقاله D=40000 و C=4 در نظر گرفته می‌شود. ضرایب مدل غیرخطی تقویت کننده مرجع (H_{ref})، در آزمایشگاه و با SNR بالا به روش کمترین مربع خطا به دست می‌آید.

البته در اینجا از [۳۱] که یک تقویت کننده توان (۲۲۴۲MAXIM MAX) را در فرکانس ۲,۴۵ گیگاهرتز اندازه‌گیری کرده و به صورت یک چند جمله‌ای ولترا بی حافظه درجه ۴ مدل کرده است، استفاده می‌کنیم و یک بردار مرجع به صورت (۸) برای شبیه سازی فرض می‌شود.



شکل ۳: الگوریتم پیشنهادی

$$H_{ref} = [h_{ref,1} \quad h_{ref,2} \quad h_{ref,3} \quad h_{ref,4}] = [32.5462 \quad 29.5342 \quad -509.5277 \quad 1311.5641] \qquad (8)$$

با گذشتن سیگنال X از تقویت کننده توان غیرخطی
با ضرایب H و عبور از کانال نویزی که نویز سفید

گوسی جمع‌شونده دارد، سیگنال ورودی گیرنده (Y) ساخته می‌شود. N برداری است که نویز کانال را در SNR مشخص، مدل می‌کند.

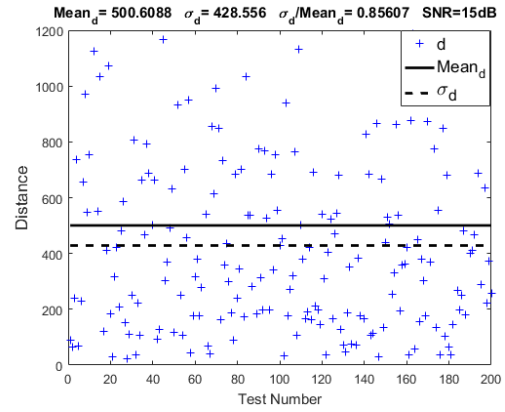
$$Y = P.H + N = \begin{bmatrix} X(n) & X(n-1) & \cdots & X(n-D+1) \\ X^2(n) & X^2(n-1) & \ddots & X^2(n-D+1) \\ X^3(n) & X^3(n-1) & \ddots & X^3(n-D+1) \\ X^4(n) & X^4(n-1) & \cdots & X^4(n-D+1) \end{bmatrix}^T .H + N \quad (9)$$

در این مرحله ماهیت H مشخص نیست و هدف این الگوریتم این است که مشخص کند آیا H ضرایب فرستنده معتبر (مرجع) است یا ضرایب فرستنده غیرمعتبر دیگری است. سیگنال Y، سیگنال گسسته‌ای است که از نمونه برداری سیگنال خروجی میکسر گیرنده به دست می‌آید. در این مرحله، سیمبول‌هایی که از Y به دست آمده است را در قالب J پاکت M تایی دسته‌بندی می‌کنیم $(J \times M = D)$. در این مقاله M=200 و J=200 در نظر گرفته می‌شود. M سیمبول اول، بردار Y_1 را می‌سازند و M سیمبول دوم، بردار Y_2 را می‌سازند و به همین ترتیب M سیمبول آخر بردار Y_J را می‌سازند. P_j ماتریسی با M سطر و C ستون است. در گیرنده با عملیات دمدولاسیون سیگنال ورودی X بازیابی می‌شود. با استفاده از سیگنال ورودی X و بردار Y_j، بردار ضرایب مدل غیرخطی (H_j) به روش کمترین مربع خطا تخمین زده می‌شود. تشریح این موضوع در [39] آمده است.

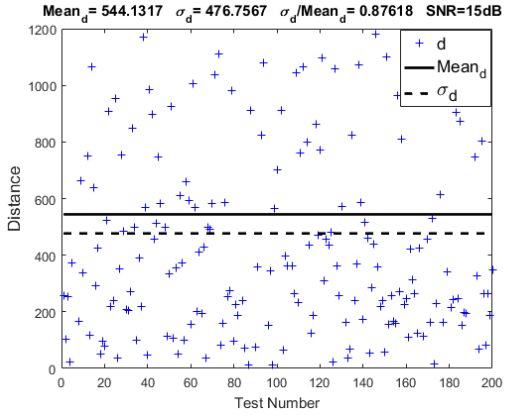
$$H_j = (P_j^* P_j)^{-1} P_j^* Y_j \quad (10)$$

ماتریس P_j^* ترانهاده مزدوج[1] ماتریس P_j است.

چهار فرآیند احراز هویت با نرم افزار مطلب شبیه-سازی شده است و نتایج چهار فرآیند احراز هویت شبیه‌سازی شده در این مقاله، در شکل‌های ۴ و ۵ نشان داده شده‌اند. برای هر تصویر J=200 آزمایش انجام شده و فاصله‌های هر آزمایش نمایش داده شده است. همچنین برای هر فرآیند مقادیر میانگین و انحراف معیار و نسبت این دو محاسبه شده است.

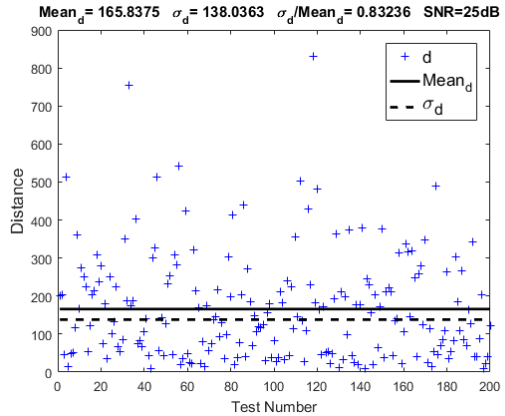


(۴- الف)



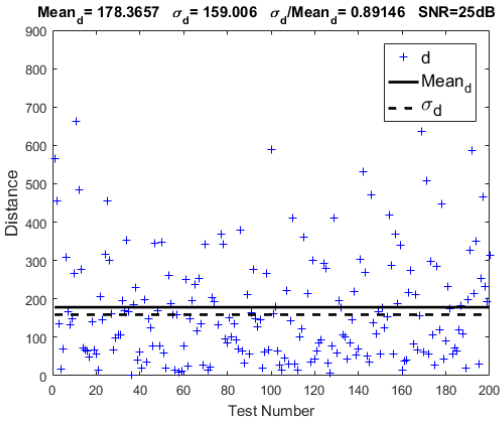
(۴- ب)

شکل ۴: فاصله اقلیدسی ضرایب مدل غیرخطی فرستنده مرجع پس از عبور از کانال با نویز تصادفی AWGN و با SNR=15dB.



(۵- الف)

[1] Conjugate Transpose or Hermitian Transpose



(۵- ب)

شکل ۵: فاصله اقلیدسی ضرایب مدل غیرخطی فرستنده مرجع پس از عبور از کانال با نویز تصادفی AWGN و با SNR=25dB.

حال فاصله اقلیدسی هر بردار H_j را با بردار H_{ref} محاسبه کرده و این فاصله را d_j می‌نامیم. در شکل ۴ و شکل ۵ این فاصله‌های اقلیدسی برای فرستنده مرجع، به ترتیب به ازای SNR=15dB و SNR=25dB نمایش داده شده است. مشاهده می‌شود که در هر عملیات شناسایی که از J=200 آزمایش تشکیل شده است، به ازای هر آزمایش، مقدار d متفاوت است. این مقادیر متفاوت به دلیل وجود کانال نویز تصادفی AWGN می‌باشد. پس این فاصله‌های اقلیدسی به تنهایی ویژگی مناسبی برای احراز هویت نمی‌باشند، زیرا مقادیر آنها وابسته به مقدار لحظه‌ای نویز کانال است. برای کاهش این وابستگی، برای هر فرستنده میانگین و انحراف معیار استاندارد ۲۰۰ فاصله اقلیدسی (J=200) به دست آمده، محاسبه شده و به عنوان ویژگی هر فرستنده ذخیره می‌شود.

پس از اینکه همه J-تا d_j محاسبه شد، میانگین d_j-ها را محاسبه کرده و m می‌نامیم. همچنین انحراف معیار d_j-ها را محاسبه کرده و σ می‌نامیم.

$$m = \frac{\sum_{j=1}^{J} d_j}{J} \quad (11)$$

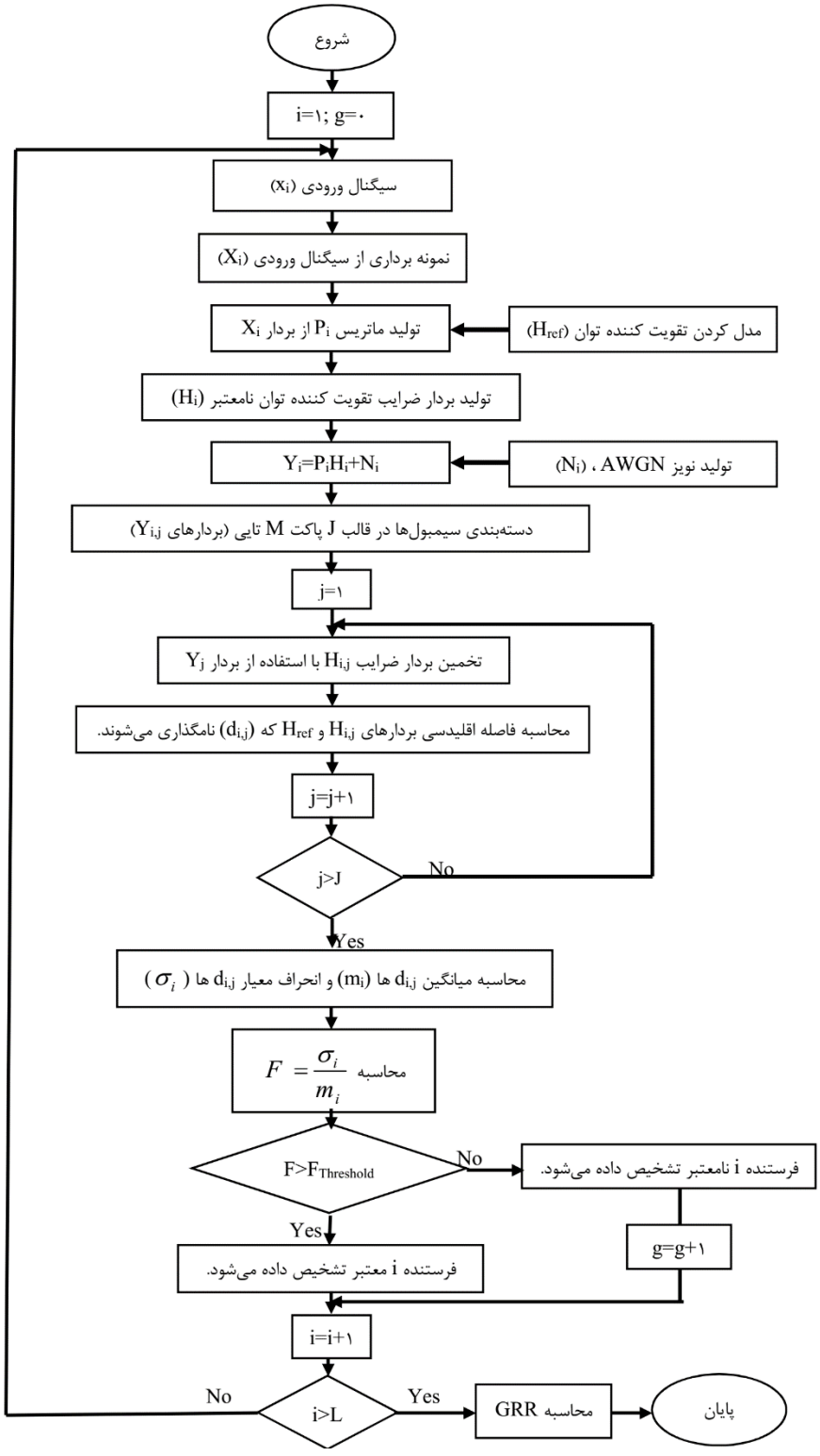
$$\sigma = \sqrt{\frac{1}{J}\sum_{j=1}^{J}(d_j - m)^2} \quad (12)$$

با مقایسه شکل ۴ و شکل ۵ مشاهده می‌شود با اینکه ویژگی‌های میانگین و انحراف معیار فاصله‌های اقلیدسی وابستگی کمی به مقدار لحظه‌ای نویز دارند، ولی این ویژگی‌ها وابستگی زیادی به SNR سیگنال دارند. بنابراین نیاز به یافتن پارامتری داریم که وابستگی کمی به مقدار لحظه‌ای نویز کانال و مقدار SNR سیگنال دریافتی از فرستنده داشته باشد، تا گیرنده بدون نیاز به اندازه‌گیری SNR سیگنال، عملیات احراز هویت فرستنده رادیویی را انجام دهد. پس با استفاده از ویژگی‌های مقادیر میانگین m و انحراف معیار استاندارد σ فاصله اقلیدسی، برای هر فرستنده پارامتری به صورت زیر تعریف می‌شود:

$$F_1 = \frac{\sigma}{m} \quad (13)$$

از این ویژگی فرستنده به عنوان معیار تصمیم‌گیری برای احراز هویت فرستنده استفاده می‌کنیم. به این صورت که اگر مقدار F از مقدار حد آستانه $F_{Threshold}$ بیشتر بود، هویت فرستنده معتبر تشخیص داده شده و در غیر این صورت، هویت فرستنده نامعتبر تشخیص داده می‌شود. شکل ۶ الگوریتم محاسبه GRR را نشان می‌دهد.

تشریح شکل ۶ مانند شکل ۳ است. در این الگوریتم L فرستنده نامعتبر مدلسازی می‌شوند و سیگنال‌های آن‌ها به گیرنده فرستاده می‌شود. در این مقاله L=۵۰۰ در نظر گرفته می‌شود. فرستنده‌های ناشناس را با استفاده از روش [۳۳] با افزودن مقادیر تصادفی تولید می‌کنیم:



شکل ۶: الگوریتم محاسبه GRR

$$H_i=[h_{i,1}\quad h_{i,2}\quad h_{i,3}\quad h_{i,4}]=H_{ref}+[0\quad \eta_{i,2}h_{ref,2}\quad \eta_{i,3}h_{ref,3}\quad \eta_{i,4}h_{ref,4}] \qquad (14)$$

که $\eta_{i,j}$ ها متغیرهای تصادفی نرمال مستقل با میانگین صفر و انحراف معیار استاندارد σ_η هستند. بر اساس [۳۳] مقدار $\sigma_\eta = 0.3$ انتخاب می‌شود. با این کار اختلاف بین تراشه‌های مختلف ناشی از خطای پروسه ساخت، مدل می‌شود. با تقسیم تعداد فرستنده‌هایی که توسط این الگوریتم نامعتبر تشخیص داده می‌شوند به تعداد کل فرستنده‌های نامعتبر (L)، GRR محاسبه می‌شود.

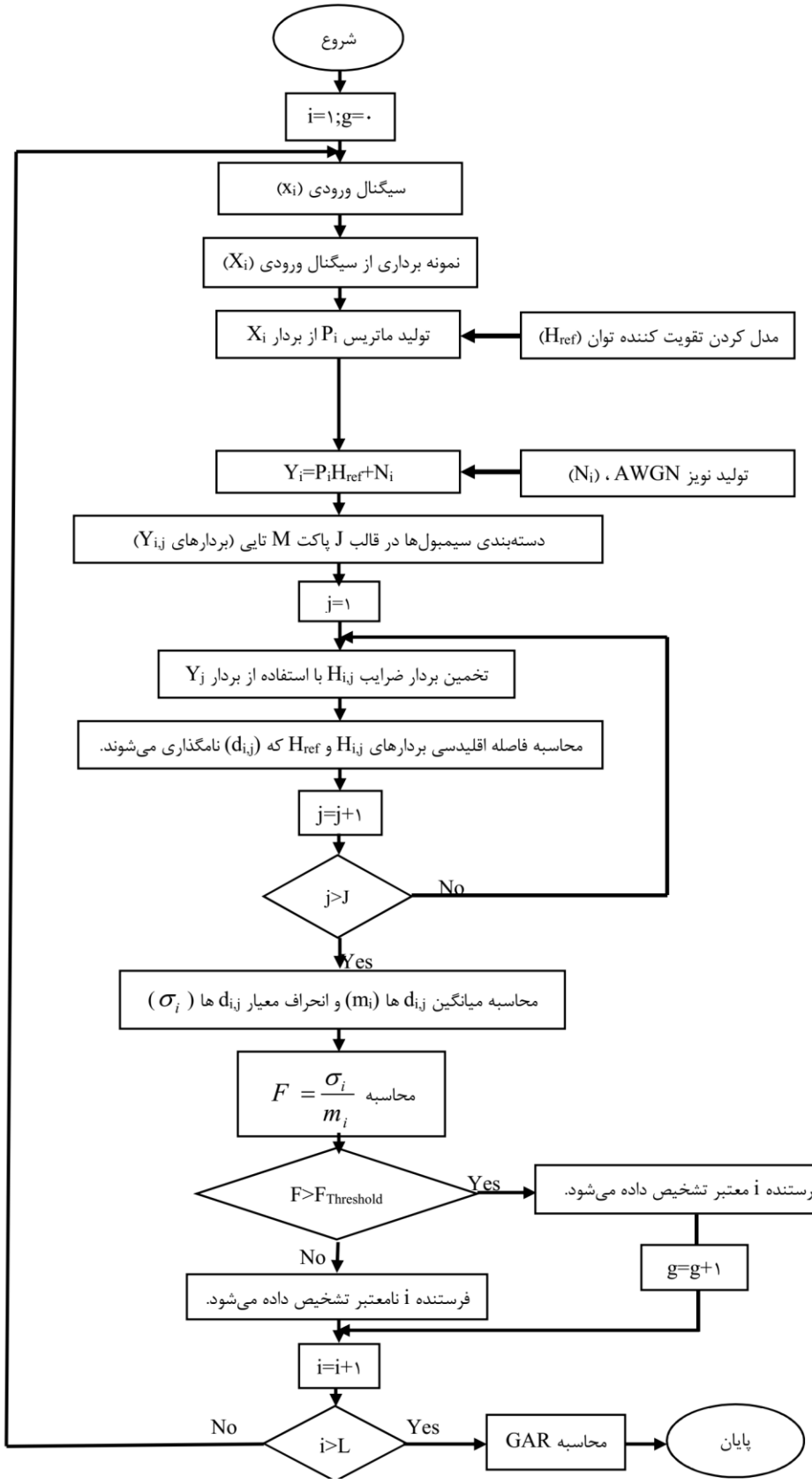
$$GRR = \frac{g}{L} \qquad (15)$$

تشریح شکل ۷ مانند شکل ۳ است. در این الگوریتم L مرتبه، سیگنال توسط فرستنده معتبر به گیرنده فرستاده می‌شود. در این مقاله L=500 در نظر گرفته می‌شود. با تقسیم تعداد دفعاتی که فرستنده مرجع توسط این الگوریتم معتبر تشخیص داده می‌شوند به تعداد کل ارسال سیگنال توسط فرستنده مرجع (L)، GAR محاسبه می‌شود.

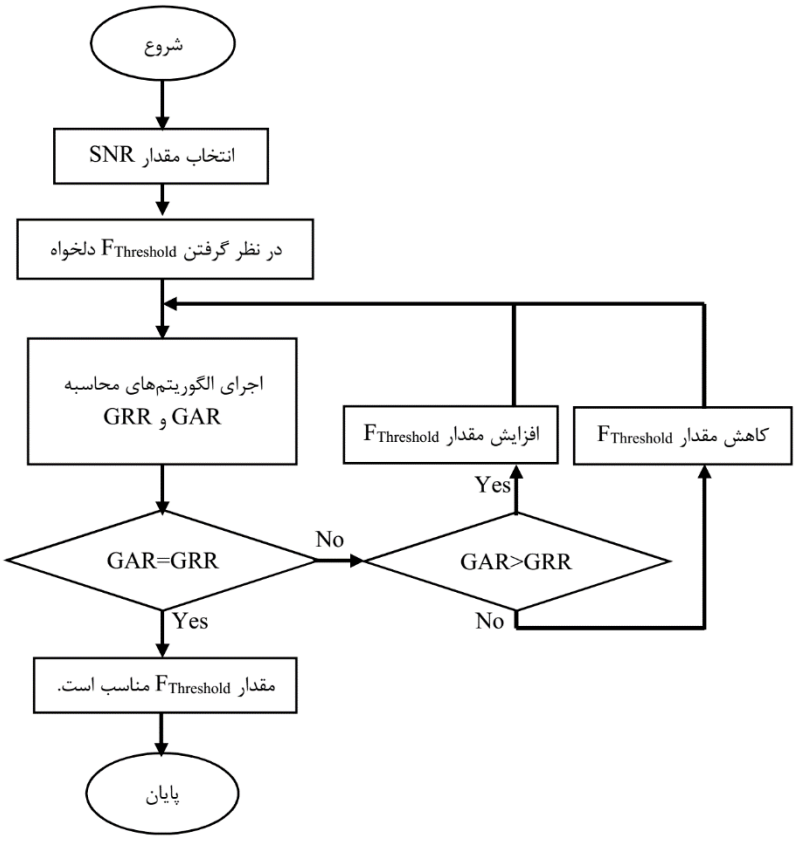
$$GAR = \frac{g}{L} \qquad (16)$$

هدف از الگوریتم شکل ۸، یافتن مقدار حد آستانه ($F_{Threshold}$) مناسب جهت احراز هویت فرستنده رادیویی در هر مقدار SNR مشخص، می‌باشد. مقدار مناسب حد آستانه، مقداری است که GAR و GRR برابر شوند.

چون در این مقاله الگوریتم پیشنهادی باید نسبت به تغییرات SNR پایدار باشد، مقدار حد آستانه‌ای که به ازای SNR=15dB محاسبه شده است، به عنوان حد آستانه برای تمام مقادیر SNR>15dB هم در نظر گرفته می‌شود.



شکل ۷: الگوریتم محاسبه GAR



شکل ۸: الگوریتم محاسبه $F_{Threshold}$ برای SNR مشخص

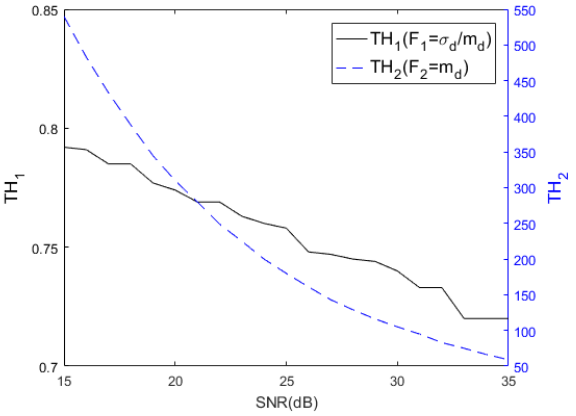
۵–شبیه سازی و ارزیابی الگوریتم پیشنهادی

برای مقایسه تأثیر *SNR* پارامتر دیگری به صورت $F_2=m$ تعریف کرده و عملیات بالا را برای آن انجام داده و نتایج را مقایسه می‌کنیم. که m همان میانگین فاصله‌های اقلیدسی است.

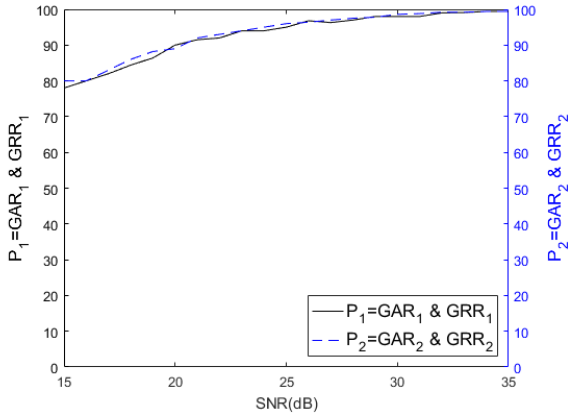
$$F_2= m \qquad (17)$$

با مقایسه شکل (۴-الف) و شکل (۵-الف) مشاهده می‌شود که به ازای 10dB افزایش SNR مقدار میانگین از 500.6 به 165.8و مقدار انحراف معیار از 428.5 به ۱۳۸ کاهش پیدا کرده است، در صورتی که پارامتر تعریف شده در معادله (۱۳) فقط از 0.856 به 0.832تغییر یافته است که به مراتب تغییر کمتری محسوب می‌شود. با توجه به وابستگی کم F_1 به مقادیر SNR می‌توان تنها یک مقدار حد آستانه برای احراز هویت در همه SNR ها از 15dB تا 35dB داشته باشیم.در شکل ۹ مقادیر حد آستانه تصمیم گیری برای احراز هویت فرستنده رادیویی که به ازای آنها احتمال پذیرش صحیح (GAR) و احتمال عدم پذیرش صحیح (GRR) سیگنال فرستنده‌ها برابر است، برای دو ویژگی تعریف شده F_1 و F_2، در SNR های مختلف رسم شده است. همچنین احتمال‌های محاسبه شده بر اساس این مقادیر حد آستانه در شکل ۱۰ رسم شده‌اند. با توجه به شکل ۱۰ اگر در هر مقدار SNR مشخص از مقادیر حد آستانه شکل ۹ استفاده کنیم، احتمال احراز هویت صحیح برای هر دو F_1 و F_2 در هر SNR تقریباً برابر است. ولی باید یک مقدار حد آستانه را انتخاب کنیم که در همه SNR ها ثابت باشد. با توجه به شکل ۹، F_1 نسبت به F_2 تغییرات بسیار کمتری نسبت به تغییرات SNR دارد. نتایج احتمال‌ها با مقدار حد آستانه ثابت برای همه SNR ها برای F_1 به ازای $F_{Threshold1}=0.792$ و برای F_2 به ازای $F_{Threshold2}=540$ (مقادیر $F_{Threshold}$ از الگوریتم شکل ۸ با SNR=15dB به دست آمده است) در شکل ۱۱ رسم شده است. همانطور که پیش

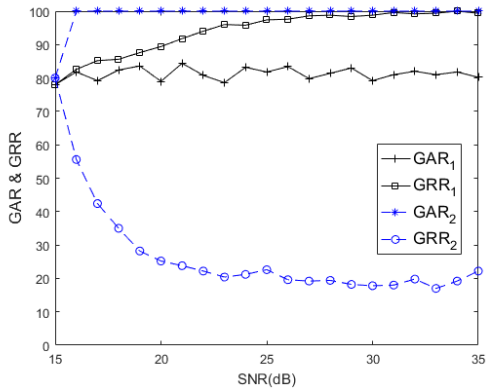
بینی می‌شد F_1 نسبت به تغییرات SNR پایدارتر است و احتمال GAR_1 حدود ۸۰ درصد است و احتمال GRR_1 با افزایش SNR از ۸۰ درصد به ۱۰۰ درصد نزدیک می‌شود، ولی F_2 به شدت وابسته به SNR است و با افزایش SNR، احتمال GRR_2 سریع از ۸۰ درصد به حدود ۲۰ درصد کاهش می‌یابد.



شکل ۹: مقادیر بهینه حد آستانه
(به طوریکه در هر SNR برای F_1 مقادیر احتمال $GAR_1=GRR_1$ و برای F_2 مقادیر احتمال $GAR_2=GRR_2$ شود.)



شکل ۱۰: مقادیر احتمال *P1* و *P2* به ازای مقادیر بهینه حد آستانه در هر *SNR*.



شکل ۱۱: مقادیر احتمال‌های *GAR* و *GRR* به ازای مقادیر حد آستانه ثابت *FThreshold1 =0.792* و *FThreshold2 =540* در همه مقادیر *SNR*.

۶–نتیجه گیری

در این مقاله احراز هویت فرستنده رادیویی بی‌سیم بر اساس ضرایب مدل غیرخطی تقویت کننده توان بررسی شد. برای اینکه معیار تصمیم‌گیری برای احراز هویت فرستنده به مقدار SNR سیگنال دریافت شده از گیرنده وابسته نباشد، یک ویژگی جدید بر اساس مشخصات آماری سیگنال دریافتی از فرستنده ارائه شد. نشان داده شد که ویژگی ارائه شده نسبت به تغییرات SNR حساسیت بسیار کمی دارد. با روش ۲۰ بار شبیه سازی انجام شد. نتایج شبیه‌سازی نشان می‌دهند که با انتخاب یک معیار ثابت تصمیم‌گیری بر اساس این ویژگی جدید که تابع SNR نیست، می‌توان فرآیند احراز هویت را با احتمال موفقیت بالای ۸۰٪ برای حداقل SNR برابر 15dB انجام داد. این روش برای شرایطی که SNR سیگنال دریافتی متغیر است، برای مثال زمانی که گیرنده یا فرستنده یا هر دو متحرک هستند، کاربردی است. همچنین عدم نیاز به اندازه‌گیری مقدار SNR، طراحی و ساخت گیرنده را ساده‌تر و کم‌هزینه‌تر می‌کند.

۷–مراجع (References)

[1] O. H. Tekbas, N. Serinken and O. Ureten, "An experimental performance evaluation of a novel radio-transmitter identification system under diverse environmental conditions," in Canadian Journal of Electrical and Computer Engineering, vol. 29, no. 3, pp. 203-209, July 2004.

[2] I. O. Kennedy, P. Scanlon, F. J. Mullany, M. M. Buddhikot, K. E. Nolan and T. W. Rondeau, "Radio Transmitter Fingerprinting: A Steady State Frequency Domain Approach," 2008 IEEE 68 th Vehicular Technology Conference, Calgary, BC, pp. 1-5, 2008.

[3] I. O. Kennedy, P. Scanlon and M. M. Buddhikot, "Passive Steady State RF Fingerprinting: A Cognitive Technique for Scalable Deployment of Co-Channel Femto Cell Underlays," 2008 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, Chicago, IL, pp. 1-12, 2008

[4] K. J. Ellis and N. Serinken, "Characteristics of radio transmitter fingerprints," in Radio Science, vol. 36, no. 4, pp. 585-597, July-Aug. 2001.

[5] R. D. Hippenstiel and Y. Payal, "Wavelet Based Transmitter Identification," Fourth International Symposium on Signal Processing and Its Applications, Gold Coast, Queensland, Australia, pp.740-724, 1996

[6] D. Shaw and W. Kinsner, "Multifractal modelling of radio transmitter transients for classification," IEEE WESCANEX 97 Communications, Power and Computing. Conference Proceedings, Winnipeg, Manitoba, Canada, pp. 306-312, 1997.

[7] M. D. Williams, M. A. Temple and D. R. Reising, "Augmenting Bit-Level Network Security Using Physical Layer RF-DNA Fingerprinting," 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, Miami, FL, pp. 1-6, 2010.

[8] F. Demers and M. St-Hilaire, "Radiometric identification of LTE transmitters," 2013 IEEE Global Communications Conference (GLOBECOM), Atlanta, GA, pp. 4116-4121, 2013.

[9] Yuan, H. L., and A. Q. Hu. "Preamble-based detection of Wi-Fi transmitter RF fingerprints." Electronics letters 46, no. 16, pp. 1165-1167, 2010.

[10] Brik, Vladimir, Suman Banerjee, Marco Gruteser, and Sangho Oh. "Wireless device identification with radiometric signatures." In Proceedings of the 14th ACM international conference on Mobile computing and networking, ACM, pp. 116-127, 2008.

[11] Rehman, Saeed Ur, Kevin W. Sowerby, and Colin Coghill. "Radio-frequency fingerprinting for mitigating primary user emulation attack in low-end cognitive radios." IET Communications 8, no. 8, pp. 1274-1284, 2014.

[12] Klein, Randall W., Michael A. Temple, and Michael J. Mendenhall. "Application of wavelet-based RF fingerprinting to enhance wireless network security." Journal of Communications and Networks 11, no. 6, pp. 544-555, 2009.

[13] Reising, Donald R., Michael A. Temple, and Julie A. Jackson. "Authorized and rogue device discrimination using dimensionally reduced RF-DNA fingerprints." IEEE Transactions on Information Forensics and Security 10, no. 6, pp. 1180-1192, 2015.

[14] Ramsey, Benjamin W., Michael A. Temple, and Barry E. Mullins. "PHY foundation for multi-factor ZigBee node authentication." In 2012 IEEE Global Communications Conference (GLOBECOM), IEEE, pp. 795-800, 2012.

[15] Hall, Jeyanthi, Michel Barbeau, and Evangelos Kranakis. "Detection of transient in radio frequency fingerprinting using signal phase." Wireless and Optical Communications, pp. 13-18, 2003.

[16] Knox, David A., and Thomas Kunz. "Practical rf fingerprints for wireless sensor network authentication." In 2012 8th International Wireless Communications and Mobile Computing Conference (IWCMC), IEEE, pp. 531-536, 2012.

[17] Danev, Boris, and Srdjan Capkun. "Transient-based identification of wireless sensor nodes." In Proceedings of the 2009 International Conference on Information Processing in Sensor Networks, IEEE Computer Society, pp. 25-36, 2009.

[18] Han, Jinsong, Chen Qian, Panlong Yang, Dan Ma, Zhiping Jiang, Wei Xi, and

[19] Knox, David A., and Thomas Kunz. "AGC-based RF Fingerprints in Wireless Sensor Networks for authentication." In 2010 IEEE International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM), IEEE, pp. 1-6, 2010.

[20] Huang, Guangquan, Yingjun Yuan, Xiang Wang, and Zhitao Huang. "Specific emitter identification based on nonlinear dynamical characteristics." Canadian Journal of Electrical and Computer Engineering 39, no. 1, pp. 34-41, 2016.

[21] Wheeler, Charles G., and Donald R. Reising. "Assessment of the impact of CFO on RF-DNA fingerprint classification performance." In 2017 International Conference on Computing, Networking and Communications (ICNC), IEEE, pp. 110-114, 2017.

[22] Peng, Linning, Aiqun Hu, Yu Jiang, Yan Yan, and Changming Zhu. "A differential constellation trace figure based device identification method for ZigBee nodes." In 2016 8th International Conference on Wireless Communications & Signal Processing (WCSP), IEEE, pp. 1-6, 2016.

[23] Pospíšil, Martin, Roman Marsalek, and Jitka Pomenkova. "Wireless device authentication through transmitter imperfections—measurement and classification." In 2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), IEEE, pp. 497-501, 2013.

[24] Suski II, William C., Michael A. Temple, Michael J. Mendenhall, and Robert F. Mills. "Using spectral fingerprints to improve wireless network security." In IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference, IEEE, pp. 1-5, 2008.

[25] Rehman, Saeed Ur, Kevin Sowerby, and Colin Coghill. "RF fingerprint extraction from the energy envelope of an instantaneous transient signal." In 2012 Australian Communications Theory Workshop (AusCTW), IEEE, pp. 90-95, 2012.

[26] Jia, Yongqiang, Shengli Zhu, and Lu Gan. "Specific emitter identification based on the natural measure." Entropy 19, no. 3, 2017.

[27] Taşcıoğlu, Selçuk, Memduh Köse, and Ziya Telatar. "Effect of sampling rate on transient based RF fingerprinting." In 2017 10th International Conference on Electrical and Electronics Engineering (ELECO), IEEE, pp. 1156-1160, 2017.

[28] Yu, Jiabao, Aiqun Hu, and Linning Peng. "Blind DCTF-based estimation of carrier frequency offset for RF fingerprint extraction." In 2016 8th International Conference on Wireless Communications & Signal Processing (WCSP), IEEE, pp. 1-6, 2016.

[29] Rubino, Riccardo. "Wireless device identification from a phase noise prospective." 2010.

[30] Azarmehr, Mahzad, Ankit Mehta, and Rashid Rashidzadeh. "Wireless device identification using oscillator control voltage as RF fingerprint." In 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE), pp. 1-4, 2017.

[31] Polak, Adam C., Sepideh Dolatshahi, and Dennis L. Goeckel. "Identifying wireless users via transmitter imperfections." IEEE Journal on selected areas in communications 29, no. 7, pp. 1469-1479, 2011.

[32] Polak, Adam C., and Dennis L. Goeckel. "Rf fingerprinting of users who actively mask their identities with artificial distortion." In 2011 Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR), IEEE, pp. 270-274, 2011.

[33] Polak, Adam C., and Dennis L. Goeckel. "Identification of wireless devices of users who actively fake their RF fingerprints with artificial data distortion." IEEE Transactions on Wireless Communications 14, no. 11, pp. 5889-5899, 2015.

[34] Polak, Adam C., and Dennis L. Goeckel. "Wireless device identification based on RF oscillator imperfections." IEEE Transactions on Information Forensics and Security 10, no. 12, pp. 2492-2501, 2015.

[35] S. S. Hanna and D. Cabric, "Deep Learning Based Transmitter Identification using Power Amplifier Nonlinearity," Jizhong Zhao. "GenePrint: Generic and accurate physical-layer identification for UHF RFID tags." IEEE/ACM Transactions on Networking 24, no. 2, pp. 846-858, 2016.

2019 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, pp. 674-680, 2019.

[36] A. S. Tehrani, H. Cao, S. Afsardoost, T. Eriksson, M. Isaksson and C. Fager, "A Comparative Analysis of the Complexity/Accuracy Tradeoff in Power Amplifier Behavioral Models," in IEEE Transactions on Microwave Theory and Techniques, vol. 58, no. 6, pp. 1510-1520, June 2010.

[37] W. Wang, Z. Sun, S. Piao, B. Zhu and K. Ren, "Wireless Physical-Layer Identification: Modeling and Validation," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 2091-2106, Sept. 2016.

[38] Hekkala, Atso, "Compensation of transmitter nonlinearities using predistortion techniques: Case studies of envelope tracking amplifiers and radio-over-fibre links." PhD Dissertation. VTT Technical Research Centre of Finland, 2014.

[39] J. Chani-Cahuana, M. Özen, C. Fager and T. Eriksson, "Digital Predistortion Parameter Identification for RF Power Amplifiers Using Real-Valued Output Data," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 64, no. 10, pp. 1227-1231, Oct. 2017.

[40] B. Danev, H. Luecken, S. Capckun, and K. El Defrawy, "Attacks on physical-layer identification," in Proc. of ACM Conference on Wireless Network Security (WiSec), pp. 89–98, March. 2010.